Title (en)

TRUSTED COMPUTING

Title (de)

SICHERE DATENVERARBEITUNG

Title (fr)

CALCUL DE CONFIANCE

Publication

EP 3198500 B1 20190501 (EN)

Application

EP 15819975 A 20151210

Priority

- US 201414587551 A 20141231
- US 2015065128 W 20151210

Abstract (en)

[origin: US2016188909A1] A trusted computing device (TCD) includes an isolated environment, host interface, secure interface, and program instructions. The environment includes an isolated environment processor (IEP), memory (secure and non-secure partition), and an auxiliary processor (AP). Memory and AP are connected for data communication with the IEP, and communicate with a host only through the IEP. The host interface and each secure interface are connected for data communication with the IEP. The instructions provision TCD for cryptographic operations via a secure interface; present a first file system partition comprising a write file and a read file with file creation/deletion privileges allocated only to the IEP at the host interface via the IEP; present a non-secured file system partition with access to the non-secure partition via the host interface via the IEP; receive, via the write file, requests to perform trusted computing; perform requested computing using the IEP, secure memory, and AP; and write results to the read file.

IPC 8 full level

G06F 21/79 (2013.01); **G06F 3/041** (2006.01); **G06F 21/35** (2013.01); **G06F 21/62** (2013.01); **G06F 21/74** (2013.01); **H04L 29/06** (2006.01)

CPC (source: EP US)

G06F 21/31 (2013.01 - US); **G06F 21/35** (2013.01 - EP US); **G06F 21/6218** (2013.01 - US); **G06F 21/71** (2013.01 - US); **G06F 21/74** (2013.01 - EP US); **G06F 21/79** (2013.01 - EP US); **H04L 63/0428** (2013.01 - US); G06F 3/041 (2013.01 - US); G06F 2221/2103 (2013.01 - US)

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

US 2016188909 A1 20160630; **US 9569638 B2 20170214**; EP 3198500 A1 20170802; EP 3198500 B1 20190501; US 10650167 B2 20200512; US 2017103234 A1 20170413; US 2018247083 A1 20180830; US 9965653 B2 20180508; WO 2016109154 A1 20160707; WO 2016109154 A8 20160825

DOCDB simple family (application)

US 201414587551 A 20141231; EP 15819975 A 20151210; US 2015065128 W 20151210; US 201615389436 A 20161222; US 201815960213 A 20180423